Solution Brief

Mobile File Sharing: Balancing Productivity, Security, and Control

Date: March 2014 **Author:** Terri McClure, Senior Analyst

Abstract: *Consumerization of IT and BYOD have IT walking a delicate line. How does IT empower employees to be productive and use the devices they want, yet keep data protected and secure? It also makes it increasingly difficult to meet compliance mandates when data is scattered across the enterprise on employees' multiple endpoint devices. It is a difficult challenge to meet, but companies like Acronis are stepping up to the plate to offer solutions that enable organizations to keep employees working the way they want while meeting security compliance requirements.*

Overview

Mobile computing is no longer a "fad"—in a recent research survey, ESG found that 32% of respondent enterprise organizations say that mobile computing is critical for supporting business processes and employee productivity; 55% claim that mobile computing is very important for supporting business processes and employee productivity; and 10% believe that mobile computing is important for supporting business processes and employee productivity. The key themes that came out of this research are that organizations need to be able to control the environment, secure the data, mobilize the end-users, and maintain balance between IT's need to be in control and users' need to be productive.[1]

However, that same report found that mobile computing is fraught with challenges. When asked to identify their top mobile computing security challenges, the most commonly identified issues included protecting data confidentiality and integrity when data is accessed by a mobile device over the network, protecting data confidentiality and integrity when data is stored on a mobile device, and enforcing security policies for mobile devices.

Protecting data confidentiality and integrity is especially important in regulated environments. When ESG studied online file sharing (OFS) in regulated environments in 2013, four out of five respondents reported that regulatory audits had taken place within the past five years, one-third reported more than five audits, and one-third of audited organizations had failed an audit in the last five years.[2] The cost of failing an audit varies by industry and can run into the hundreds of thousands of dollars, depending on the severity of the issues found.

Among these regulated industries, secure corporate online file sharing and collaboration solution adoption is strong, with 46% reporting they've deployed corporate solutions. But rogue OFS utilization, (employees using personal OFS accounts rather than the corporate-provided solution) is prevalent with 60% of respondents knowing or suspecting it is taking place. And even though 92% of organizations formally or informally discourage rogue OFS use, nearly 70% of respondents knowing/suspecting rogue OFS utilization report it is *likely that regulated data has been stored in rogue OFS accounts.*[3]

It is critical for IT organizations to address the rogue OFS usage problem, get regulated data out of personal OFS accounts, and secure mobile data. These personal accounts are used by employees for a number of reasons, but mostly because it is an easy way for them to access and share files via mobile devices, and it enhances their productivity. As shown in the mobile computing survey, this balance between control, security, and productivity is critical. The answer is for IT organizations to carefully evaluate online file sharing and collaboration solutions that enable them to attain this balance—solutions that are easy for end-users to use, with full accountability for IT.

[1] Source: ESG Research Report, *The State of Mobile Computing Security*, February 2014.
[2] Source: ESG Research, *OFS Considerations in Highly Regulated Industries*, June 2013.
[3] Source: Ibid.

What Users Look for in an OFS Solution

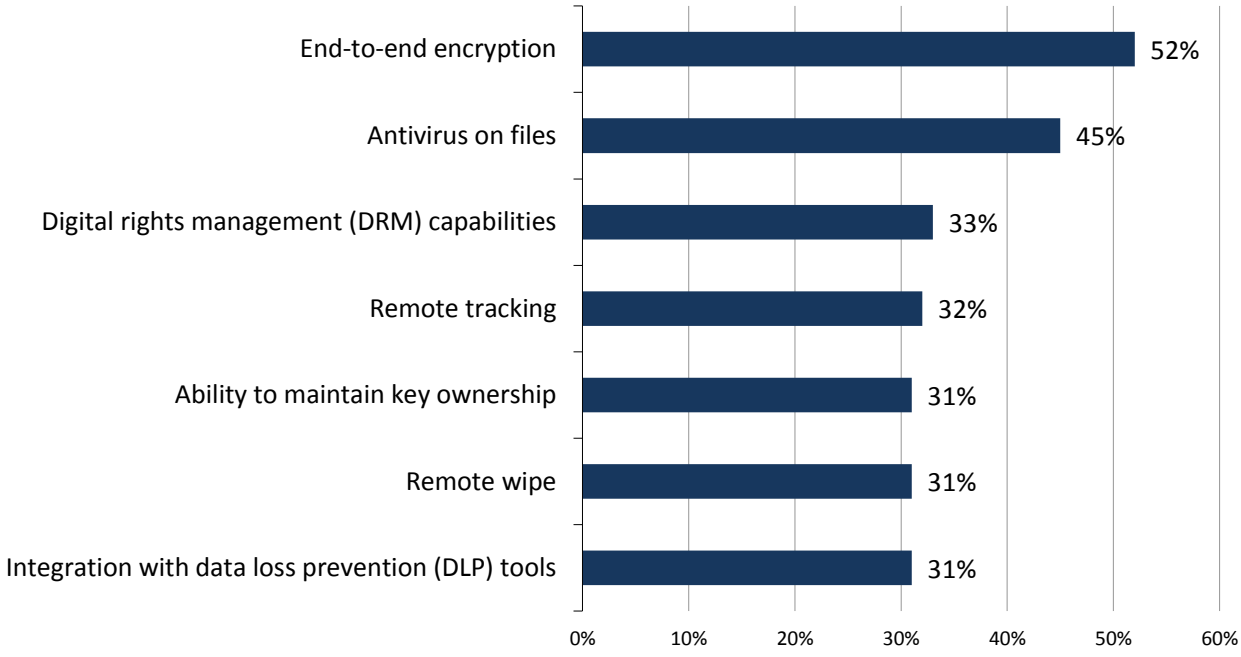
Plenty of solutions out there claim to be as easy to use as the most popular consumer solutions while providing security and control for IT—but what is really required to achieve this balance? Ease of use is certainly important because if the OFS solution isn't easy to use, then rogue usage continues. In fact, in more recently conducted research, one in four professionals responsible for their organization's file sharing environment indicated that a key challenge with their corporate OFS accounts is that users continue to use their private accounts for business.[4] One sure driver for that is the ease of use of the consumer solution, and end-users' familiarity with how it works.

In that same survey, IT pros were asked about key OFS feature requirements in general and security features in detail. General feature requirements largely coincide with fitting into existing business process and workflows. The top three features (each with 31% of respondents) are integration with existing applications, ability to sync across multiple device types, and scalability. Reflecting users' concerns about accountability, integration with auditing software and tools is close behind. And when ESG asked users about choosing solutions specifically, ease of use for end-users was a top requirement, with more than one in four citing it as one of their most important criteria. So the first part of the balancing act is: can the solution plug into the existing IT environment; is there auditability; can it support different types of endpoints; and is it easy enough to use that end-users will stop using their personal accounts for business data?

The second part of the equation is where it gets tricky: keeping data in an OFS solution secure (yet maintaining ease of use). When vendors start layering in security functionality, the solutions can get complex—but if OFS data is to be secured, then these features are core requirements, specifically encryption to make sure prying eyes can't see readable data; antivirus because data from so many users is shared and can quickly spread a virus; and the ability to maintain key ownership so that no third party can access the keys and crack the encryption (see Figure 1). The list goes on, but for regulated environments, audit logs and reports are certainly a core requirement to ensure nobody has tampered with, accessed, or shared data they shouldn't have.

Figure 1. Top Five Corporate OFS Security Requirements

Which of the following security-specific requirements does your organization require from a corporate online file sharing and collaboration service? (Percent of respondents, N=334, multiple responses accepted)



Source: Enterprise Strategy Group, 2014.

[4] Source: ESG Research Report, *Online File Sharing and Collaboration: Deployment Model Trends*, February 2014.

Again, the key here is adding those features and maintaining usability for end-users so that they stop using personal accounts. This is not an "***or***" discussion—it is not about integrating with the existing applications ***or*** making it easy to use ***or*** making it secure. This is an "***and***" discussion—IT needs a solution that integrates with the existing environments ***and*** is secure ***and*** easy ***and*** full featured ***and*** provides accountability for how data is accessed and used. That is where many solutions falter—it is extremely difficult to build a solution that maintains ease of use and does everything else IT wants.

Acronis Access: Balancing Control, Security, Compliance, and Productivity

Acronis has just such a solution. It is designed to work within an enterprise IT environment with features such as active directory integration. It meets security requirements by enabling administrators to:

- Set policies for operations such as which applications can be used to open, view, and edit files.
- Secure and expire links.
- Limit whether files can be synced to or cached on mobile devices.
- Enforce smart card two-factor authentication (CAC/PIV).

It helps enable compliance with:

- Audit log and FIPS 140-2.

It helps streamline productivity with:

- Easy-to-use clients that span the cornucopia of device types in use today.
- Role-based administration that puts administration responsibilities into the hands of the people who know the business process: departmental administrators.
- Edit and create office documents and annotate PDFs within the encrypted Acronis environment.
- Distribute content via one-way sync, which automatically syncs latest versions of files to a specific audience.

Of course, the Acronis Access solution has more functionality, but this is a sampling of the features that allow Acronis to help IT walk the line of enabling employee productivity in a secure and compliant way.

The Bigger Truth

With the influx of consumer devices in the workforce, it is not surprising that consumer applications are making their way into the workforce as well. But the risk of having employees use these solutions for regulated or sensitive information is unacceptable. IT must put solutions in place that allow them to secure and control corporate data.

IT must find the balance between control, security, compliance, and employee productivity. It needs to deploy solutions that are easy enough to use that employees can pick them up intuitively and with minimal training, just like the consumer tools they use at home. However, these solutions must also provide the proper security and protections required for corporate data. In regulated environments, solutions need to provide control and accountability that enables IT to ensure the right people have the right access to the right data; make sure data is secured, retained, and kept in its original form; and provide the reporting to prove it.

As evidenced by its robust product set, Acronis certainly understands these needs. It has developed a product well suited for today's mobile enterprise—one that walks the delicate line between security and productivity.